Ahmad Yousuf

Portfolio Project 2

07/13/2025

Threat Hunting with MITRE ATT&CK

Objective

Conduct a structured threat hunting exercise using the MITRE ATT&CK framework to identify suspicious patterns in log data and document findings in a formal report.

Background and Motivation

Threat hunting is a proactive cybersecurity practice that involves searching for threats that evade traditional detection. The MITRE ATT&CK framework provides a structured approach to identifying adversary behavior based on real-world techniques. This project applies ATT&CK techniques to log data from a Windows system to uncover suspicious activity.

Scope

- Focused on log analysis using MITRE ATT&CK techniques
- Investigated four techniques: command-line abuse, credential misuse, network scanning, and PowerShell exploitation
- Documented findings in a structured report
- No live incident response or automation involved

Tools and Technologies

- MITRE ATT&CK Navigator
- Splunk
- Sysmon and Windows Event Logs
- PowerShell
- Markdown or Excel for reporting

Threat Scenario Summaries

Technique: T1059 – Command and Scripting Interpreter

- Detected suspicious use of PowerShell with base64-encoded commands
- Parent process was explorer.exe, suggesting interactive use
- Activity matched known adversary behavior

Technique: T1078 – Valid Accounts

- Multiple successful logins from the same account across different IPs
- Occurred outside normal hours
- Indicative of credential misuse

Technique: T1046 – Network Service Scanning

- One IP scanned over 50 ports on a single host in 2 minutes
- Included both common and obscure ports
- Consistent with reconnaissance behavior

Technique: T1086 – PowerShell

- PowerShell used to download remote file and create persistence
- Executed by a standard user account
- Matched malicious scripting patterns

Challenges and Solutions

- High log volume required precise filtering
- Mapping ATT&CK techniques to log events took careful study
- False positives mitigated by correlating with known user behavior

Security Considerations

- Analysis conducted in isolated lab
- Logs anonymized and preserved
- No production systems affected

Conclusion

This project demonstrated how MITRE ATT&CK can guide effective threat hunting. Suspicious activity was identified across multiple techniques, and findings were documented to support future detection efforts.

References

- MITRE ATT&CK: https://attack.mitre.org
- Splunk Docs: https://docs.splunk.com
- Sysmon: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon